UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,157	11/03/2003	Robert N. Nazzal	12221-026001	5548

26161 7590 05/16/2008
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
GEE, JASON KAI YIN	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** *10/701,157*	**Applicant(s)** NAZZAL, ROBERT N.
	Examiner JASON K. GEE	**Art Unit** 2134

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 02 May 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) ☐ The period for reply expires ______months from the mailing date of the final rejection.

b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a)☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b)☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d)☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Continuation of 11. does NOT place the application in condition for allowance because: In regards to claim 1, the applciants argue that the prior art does not include a field that depicts a summary of anomalies identified as part of a event. However, this is indeed taught by the reference. As seen in the previous art rejections, Figure 26, paragraph 514, the abstract, and paragraph 42 of Cooper teaches this. As seen in Figure 26, a summary of all the anamolies are shown, such as access violations and security attacks. Further, the applicants argue that the prior art does not teach a 'snooze' function. However, in the previous office action, this is addressed. The remember command allows an action to continue and prevents an alert from appearing in the future. This is exactly equivalent to snoozing future alerts related to the event for a period of time. The appellant argues that this does not operate for a period of time. However, Symantec does teach this. Although Symantec may not teach how long the period of time is, Symantec does teach snoozing the alerts for some amount of time. The claim is not limited to a period of time. The appellants also argue that there is no motivation to combine. However, both the references are geared toward security, such as thorugh virus and intrusion prevention. It would be obvious to combine such relevant art, as it would increase security. As per claim 2, paragraph 100 and 158 teaches applying rules based on events and and hosts. Symantec is the used to teach it would be obivious to allow alerts relating to such rules and policies to be snoozed/remembered. In regards to claim 4, the applicant argues that the arguments poitn to claim 12 and nothing is showed. FIgure 12 is a typo, and it should have read 22. However, this was in the rejection itself, which the appellent did not read. The rejection for claim 4 points at figure 22, and it clearly shows anomlies that classify events. As per claim 10, the applicants argue that the Billhartz combination does not teach the claimed limtations. Howeer, the Billhartz combination does teach this, as addressed in the previous office action. Billhartz teaches that intrusion alerts may be generated after a threshold percentage is reached. This would create a corresponding alert. In the most broad interpreation, there are two types of event severity: no problem oat all, or a problem. An indication of an intrusion means there is a problem. Further, as shown in Figure 22 of COoper, it is shown that tehre are many different types of event sevirity. It would be obvious to combine the teachigns of Cooper with Billhartz to teach this as it would increase security and efficiency. As per claim 18, the appellnt argues that Cooper does not teach displaying the role classificaiton of the host in the network. HOwever, Cooper already teaches in paragraphs 100 and 158 that rules may be based on role classificaiton. Cooper then teaches throughout the reference that these rules may be displayed, and thus, role classifcaiton would be displayed as they are used in rule policy generation.